94

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/066,140	02/01/2002	Satyendra Yadav	10559-755001	5189

20985 7590 06/20/2006

FISH & RICHARDSON, PC
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
PERUNGAVOOR, VENKATANARAY	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 06/20/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/066,140	**Applicant(s)** YADAV, SATYENDRA	
	Examiner Venkat Perungavoor	**Art Unit** 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 May 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30,34 and 35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *31-33* is/are allowed.

6)☒ Claim(s) 1-30 an 34-35. is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date [illegible]

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. The Applicant's arguments filed 5/8/2006 are not persuasive. As Moran(U.S. Patent 6,996,843 B1) discloses the detection based on authorized requests see Col 12 Ln 46-60 (mentions the privileged user and unprivileged user uses for detection of intrusions). In order for the IDS to make an distinction between privileged and unprivileged user it must understand that it is an authorized request. And further, Moran mentions the system checking of privileges see Col 25 Ln 50-62. And also Moran discloses the using the signature of a file(applications are included) for checking purposes and policy institution see Col 4 Ln 13-20.

2. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 102

3. Claim 1-30, 34-35 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent 6,996,843 B1 to Moran.

4. Regarding Claim 1, Moran discloses the receiving of requests from an invoked application see Col 7 Ln 27-32; selectively designating request as authorized or unauthorized see Col 7 Ln 34-38; monitoring inbound communications to detect intrusion see Col 9 Ln 24-33.

5. Regarding Claim 2, Moran discloses the blocking of inbound network communications that fail the authorized request see Col 7 Ln 39-49; monitoring the blocked network communications to detect intrusion see Col 8 Ln 25-48.

6. Regarding Claim 3, 14, 27, 33, Moran discloses the examining the communications, identifying the source, and initiating monitoring of communications see Col 9 Ln 14-33.

7. Regarding Claim 4, Moran discloses the checking for patterns spanning multiple communications see Col 10 Ln 8-14.

8. Regarding Claim 5, 17, Moran discloses the generating of fabricated response see Col 1 Ln 65-16.

9. Regarding Claim 6, 29, Moran discloses the checking the communications for packet-level exploits see Col 14 Ln 35-46.

10. Regarding Claim 7, 18, Moran discloses the increasing of the level of monitoring in response to exploits see Col 8 Ln 37-48.

11. Regarding Claim 8, Moran discloses the monitoring using a application-specific signature see Col 8 Ln 11-16.

12. Regarding Claim 9, 15, 28, Moran discloses the examining the set instructions of the application see Col 13 Ln 12-42.

13. Regarding Claim 10, Moran discloses the intrusion detection system invoked with the invoked application see Col 21 Ln 4-16.

14. Regarding Claim 11, 20-21, Moran discloses the applications and intrusion detection run within the single execution context see Col 32 Ln 55-65 & Col 24 Ln 56-67.

15. Regarding Claim 12, 19, 30, Moran discloses the applying of hash to a set of instructions and comparing of the hash see Col 31 Ln 66- Col 32 Ln 3 & Col 32 Ln 55-65.

16. Regarding Claim 13, Moran discloses the receiving of requests from an invoked application see Col 7 Ln 27-32; selectively designating request as authorized or unauthorized see Col 7 Ln 34-38; monitoring inbound communications to detect intrusion see Col 9 Ln 24-33; the blocking of inbound network communications that fail the authorized request see Col 7 Ln 39-49; monitoring the blocked

network communications to detect intrusion see Col 8 Ln 25-48; the monitoring using a application-specific signature see Col 8 Ln 11-16.

17. Regarding Claim 22, Moran discloses the application network enforcer which serves application invoked on a machine, identifies the network request that fail to satisfy policy and that satisfy policy see Col 10 Ln 15-33; the blocking of inbound network communications that fail the authorized request see Col 7 Ln 39-49; monitoring the blocked network communications to detect intrusion see Col 8 Ln 25-48.

18. Regarding Claim 23, Moran discloses the examining the communications, identifying the source, and initiating monitoring of communications see Col 9 Ln 14-33.

19. Regarding Claim 24, Moran discloses the receiving of requests from an invoked application see Col 7 Ln 27-32; selectively designating request as authorized or unauthorized see Col 7 Ln 34-38; monitoring inbound communications to detect intrusion see Col 9 Ln 24-33; the examining the communications, identifying the source, and initiating monitoring of communications see Col 9 Ln 14-33.

20. Regarding Claim 25, Moran discloses the generating of fabricated response and responding to the intrusion see Col 1 Ln 65-16.

21. Regarding Claim 26, Moran discloses the receiving of requests from an invoked application see Col 7 Ln 27-32; selectively designating request as authorized or unauthorized see Col 7 Ln 34-38; monitoring inbound communications to detect intrusion see Col 9 Ln 24-33; the examining the communications, identifying the source, and initiating monitoring of communications see Col 9 Ln 14-33; the monitoring using a application-specific signature see Col 8 Ln 11-16.

Allowable Subject Matter

22. Claims 31-33 are allowed. The Applicant's amendment recites detecting communication activities including scans and fingerprinting with a fabricated response detection system is not found in prior art.

Conclusion

23. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a). A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the

advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

24. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Venkat Perungavoor whose telephone number is 571-272-7213. The examiner can normally be reached on 8-4:30. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

25. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Venkat Perungavoor
Examiner
Art Unit 2132

VP
6/14/2005

GILBERTO BARRON Jr
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100